Chapter 303

INFORMATION SYSTEMS AND TECHNOLOGY

Introduction

The Information Systems and Technology (IST) program provides information services needed to effectively manage the corporate. Hence, the board of directors and senior management must determine what information is needed to make informed decisions and monitor activities of the corporate. From this point, systems must be developed to ensure that the desired information is usable as performance measurements.

A corporate's IST program should be designed to:

1. enhance communication;
2. deliver complex material throughout the corporate;
3. provide an objective system for recording and aggregating information;
4. provide timely and reliable information for services provided to the membership;
5. reduce expenses related to labor-intensive manual activities;
6. support the organization's strategic goals and directions; and
7. provide effective interface capabilities among separate systems.

The five components listed below are essential in considering the usability of any IST program. Management decisions and strategies may be rendered invalid or detrimental if any one of these components is compromised.

Examiners must review the following components during the examination:

1. Timeliness - Information must be current and available to all appropriate users to facilitate timely decisions. This necessitates prompt collection and editing of data.

2. Accuracy - A sound system of internal controls must be in place to ensure the accuracy of data. Information should be properly edited

and reconciled with the appropriate control mechanisms in place. A comprehensive internal and external audit program would greatly facilitate this endeavor.

3. Consistency - Consistency is needed to ensure data provided is valid, as it is relied upon in making decisions and evaluating strategies. Variations in how data is collected or reported can distort trend analysis. Any change in collection or reporting procedures should be clearly defined, documented, and communicated to all users.

4. Completeness - Information input into IST must be complete.

5. Relevance - Information provided must be relevant. Details which are inappropriate, unnecessary, or unsuitable are of no value in effective decision making.

Decision makers cannot fulfill their responsibilities unless all pertinent information is provided in a comprehensive, yet concise format.

Care should be taken to ensure senior management and the board of directors receive relevant information in order to identify and measure potential risks to the corporate. Sound IST procedures are a key component of management effectiveness and should be evaluated in relation to the size, structure, and decision-making process of each individual corporate.

Advances in technology have helped corporates improve both information availability and models for analysis and decision making. Regardless of the technology employed, it is management's responsibility to develop an information system which facilitates the corporate's activities.

An effective IST program draws information from a number of sources for users with various needs. An IST program must selectively update information and coordinate it into meaningful and clear formats. A realistic approach would be to integrate a corporate's accounting system with other resources such as: information regarding economic conditions, characteristics of the market place, competitors, technology, legal/regulatory requirements, et cetera.

Processing Environment

The increasing reliance on automated system technologies by corporates has significantly increased the risk of financial losses due to inaccurate recordkeeping, unauthorized access to financial and members' records, interruption of member service, or fraud. These risks are increased further by the growing use of on-line systems, microcomputers, local area networks, and remote access to records. As a result, the growth of these automated technologies has expanded the scope of IST risk to include all user areas of a corporate.

In general, corporates have a number of choices available to meet their data processing needs. They include: installing an in-house computer center, using a service bureau, or contracting with a facilities management company to manage an existing in-house computer center. Regardless of the type selected, it is essential the board of directors and management establish appropriate policies, procedures, and controls over data processing activities to ensure the accurate processing of information, the privacy of financial and members' records, and the continuation of service in case of disasters.

In-house Computer Center

In-house computer systems vary in size and complexity according to the size of the corporate, the number of applications processed, the transaction volume, and processing deadlines. Computer equipment may vary in size from large "main frame" systems to smaller minicomputers installed as a "turnkey" system. In the turnkey system, a vendor company installs and tests the computer software before the system is turned over to the customer. Software for in-house computer systems may be developed in house or purchased from outside vendors.

Some IST risk areas posed by using an in-house computer system are inadequate hardware and software systems, excessive cost, lack of internal controls, inaccurate financial and customer data, unauthorized access to data processing files, and lack of a disaster contingency plan.

NOTE: The majority of corporates have either an in-house system or minicomputers installed as a "turnkey" system. In most cases, the Corporate Credit Union Network (CCUN) system is the main data system used by corporates. The CCUN system is expected to be replaced in the near future.

Information Security Risk Assessment

Corporates must maintain an ongoing information security risk assessment program that effectively gathers data regarding the technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards, and requirements. The program should analyze the probability and impact associated with the known threats and vulnerabilities to its assets and prioritize the risks present to determine the appropriate level of training, controls, and testing necessary for effective mitigation.

Firewalls

Firewalls are an essential control for a corporate with an Internet connection and provide a means of protection against a variety of attacks. Firewalls should not be relied upon, however, to provide full protection. Corporates should complement firewalls with strong security policies and a range of other controls. Corporates can reduce their vulnerability to attacks somewhat through network configuration and design, sound implementation of its firewall architecture, and intrusion detection systems.

Corporates have a variety of firewall options to choose from depending on the extent of Internet access and the complexity of the network. Based on system complexity, consideration of firewall options should include the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

Intrusion Detection

Corporates should have the capability to detect and respond to an information system intrusion commensurate with the risk tolerance

established by the board of directors. Preemptive practices should include the analysis of data flows, decisions on the nature and scope of monitoring, and the development of appropriate policies governing detection and response. The response to an intrusion should include the containment and restoration of systems and appropriate reporting to senior management and officials.

Controls

There are basic controls which must be present in any level of computer operations. These controls should be present at the data center. The evolution of microcomputer-based systems has not eliminated the need for basic controls; rather it has increased the focus of control at the end-user level.

IST controls prevent, detect, correct, and enable recovery from problems that can result from accidents, errors, misuse, sabotage, loss of equipment, loss of data, and any other occurrence that may lead to an unwanted or unexpected disruption of service. The three major categories of IST controls are 1) management controls, 2) general controls, and 3) applications controls.

Management Controls

The reviewer should have a good understanding of how a corporate manages its information systems and services it provides to its members. Similar control issues exist for this area and those generally found in other operational areas, and they require similar review procedures. Good IST management includes:

1. Organization. A corporate should have a well-defined organizational structure that includes the IST department or service area. Ideally, corporates should establish IST as a separate entity that reports directly to management and not through another department. The IST department should maintain an up-to-date topology (a visual representation of the hardware layout) to describe how various systems interact and share data.

2. Planning. The corporate's short- and long-term plans should identify management's direction regarding its IST operation. Management should regularly document, update, and review these plans, which should include well thought out designs for installation of new systems and modification of existing ones.

3. Policies and Procedures. Policies and procedures must be in writing and should define steps to be taken to protect the corporate's computer systems. Management should designate responsibility within the corporate to monitor the acquisition and use of computers. The policy should ensure the required degree of compatibility exists among hardware and software systems throughout the corporate.

4. Monitoring Operations. The crucial oversight function of IST operations can involve the use of committees such as an IST management committee, IST steering committee, or the supervisory committee.

5. Audit. Auditing the IST area is a cost of doing business. Corporates should require regular internal and external reviews of IST operations and services.

General Controls

General control issues exist in any automated environment and remain essential to the day-to-day operation of any IST system. General controls are not specific to any one application or function. General controls should address the following areas:

1. Organizational. The corporate should establish and maintain separation of duties which is a key element of any IST operation. Good internal controls prevent any single employee from having control over the input, processing, and output of transactions. A compensating control, in smaller corporates, could be frequent and detailed review of transaction logs. Other important areas include employment procedures, job descriptions, security statements to help control data, and termination procedures.

2. Data center management. The operation of the data center includes the control and scheduling of input and output, problem prevention and correction, and reporting. Procedures should be in place and up-to-date for each of these areas.

3. Software controls. Corporates must control access to software by unauthorized persons, especially the control and use of the operating system, software utilities, communications, and security software. System logs are useful tools for monitoring activity and changes to the system if management produces and reviews them regularly.

4. Hardware controls. Corporates should document and enforce external controls on hardware including: access controls, terminal usage, and system support and service. Computers have internal hardware controls including: validity, parity, and echo checks that most users do not see. These hardware controls monitor and check for proper hardware function.

5. Physical security. The computer room should have evidence of physical controls including: access controls and logs, fire and theft protection, terminal access controls, and protection of data files and media. Log-on procedures, user IDs, passwords, and physical or electronic keys will provide additional access control to the system.

6. System design, development, modification, testing, and implementation. Corporates should document the methods and procedures for developing and testing new and enhanced systems.

7. Contingency plan. The ability to retain, restart, and replace activity quickly is an important control feature of any IST system. A well-run and controlled operation includes a written and tested contingency plan, proper backup and recovery actions and procedures, and management's commitment to contingency planning.

Application Controls

Application controls apply to the processing of data into, through, and out of the system. An awareness of IST controls enhances the review of automated parts of the process. A third-party review of this area is recommended in most corporates. Application controls consist of the following:

1. Data origination. Basic controls of data origination include batch totals, control totals, turnaround documents, and retention of source documents. Source documents should be designed for easy and accurate data input.

2. Data input. Controls of data input include conversion, validation, editing, error handling, and separation of duties.

3. Data processing. External controls maintain the operation of the system until completion of the application processing. These controls include system start-up procedures, backup and emergency procedures, error message debugging, and system and job status reporting. Internal validation and editing routines built into the programming checks for errors. The corporate should have error handling procedures to identify and correct transaction errors.

4. Data output. Balancing and reconciliation, distribution, error handling, and records retention procedures complete the application processing function.

Backup and Recovery

Corporates should regularly and routinely backup computer data. Several considerations involving backup and recovery of information include:

1. Frequency. Corporates should backup data files at least daily; application files both when they make changes and routinely, usually monthly or quarterly; a current copy of the operating system, and vital records every three months.

2. Generations. Many corporates keep five sets of data file backups, one made each day of the week.

3. Storage. Corporates must store vital records off-site, at a location far enough from the offices, to avoid the simultaneous loss of both sets of records. Corporates should keep backup files both on- and off-site. Any off-site set of tapes should be encrypted for additional security.

4. Management. Corporates should routinely control, maintain, and test backup files for quality and accuracy.

5. Recovery. Corporates should address and document relevant issues including the speed of data file recovery, who can recover them, and under what conditions.

Contingency Planning

Restoring operations to an acceptable level within a reasonable amount of time requires that all corporates using any type of IST services have a comprehensive, written, accurate, up-to-date, tested contingency plan. Responsibility for developing this plan lies with management of the corporate. Refer to Chapter 307 – Contingency Planning for further information.

Audits

The audits of the IST area, including both internal and external reviews, give the corporate assurance that the system's design and operation function is as intended. Internally, the corporate should perform, at a minimum, quality and accuracy checks on the system's processing to ensure the presence of at least the minimum control requirements for each type of system in use. Depending on the complexity of the IST systems, a corporate may need a complete third-party audit. In addition, external and internal penetration assessments should be performed. Complex corporates may need an internal IST auditor to perform routine, recurring reviews of the system.

Outsourcing

Corporates often rely on third parties to provide and support technology-related functions and services. Outsourcing arrangements can help manage costs, provide expertise, as well as expand and improve services offered to members. Corporate management ultimately remains responsible for managing the risks associated with the system or service.

Corporate management is responsible to ensure member data is protected, even when the data is transmitted, processed, or stored by a third-party provider. Third-party providers should have appropriate security testing based on the risk to the organization. Corporate management is responsible for monitoring the testing performed by the third-party provider through review of timely audits and test results or other evaluations.

Security and Privacy

Part 748 of the NCUA Rules and Regulations requires each federally-insured credit union to develop a written security program. This program must strive to:

- Protect each credit union office from robberies, burglaries, larcenies, and embezzlement;
- Ensure the security and confidentiality of member records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to the member;
- Assist in the identification of persons who commit or attempt such actions and crimes; and
- Prevent destruction of vital records, as defined in 12 CFR Part 749.

The appendix to Part 748 provides guidelines to assist credit unions in meeting the above four criteria. The guidelines provide a good framework from which a corporate credit union can work to develop their policies and procedures.

Security Policies and Procedures

The corporate should consider the following when developing security policies and procedures:

- Identifying the services provided and systems (hardware and software) used;
- Identifying the risks and threats associated with each system and service;
- Determining the likelihood the risk or threat could occur;
- Identifying and evaluating various methodologies to mitigate the risks or threats;
- Developing the policies and procedures to address the risks or threats;
- Monitoring, and adjusting if necessary, the policies and procedures to achieve the desired results;
- Reviewing policies and procedures at least annually; and
- Training and educating staff.

Operations Impact

Corporate examiners should consider the following when assessing the IST area:

1. Strategic Plan & Goals:
    a. Has management developed a strategic plan for the corporate's IST systems and services?
    b. Has management developed strategic goals, policies, and procedures to implement the strategic plan?
    c. Are those strategic goals, policies, and procedures adequate? They should consider at least, the following items:
        i. Size and complexity of the corporate;
        ii. Types of services offered;
        iii. Volume of IST activity;
        iv. Member demand, usage, and expectations, and
        v. Criticality of systems and services

Critical or non-critical. Management must determine whether IST systems and services are critical or non-critical to the corporate's

operations. Management should base this determination on factors including: risk exposure (transaction, security, compliance, reputation, etc.), type of services offered, transaction volume (number and dollar), interconnectivity impact with other systems, member usage, and member expectations and perceptions.

2. Risk Analysis:
    a. Has management performed a risk analysis? The analysis should include at least the following considerations:
        i. Assessment;
        ii. Impact analysis/evaluation;
        iii. Mitigation;
        iv. On-going/periodic monitoring; and
        v. Reporting procedures

3. Policies:
    a. Has management developed appropriate and adequate policies? The policies should address at least the following points:
        i. Security;
        ii. Compliance;
        iii. Business continuity;
        iv. Disaster recovery; and
        v. Vendor management

4. Oversight:
    a. Does management provide adequate oversight? The oversight should include at least the following items:
        i. Adequate staffing;
        ii. Knowledgeable/informed staff; and
        iii. Adequate reporting procedures at various management levels
    b. Has the internal and/or external review program been modified to include reviewing procedures for IST activity?
    c. Does management address issues/concerns effectively, adequately, and timely?
    d. Does management have adequate vendor oversight policies, procedures, and practices?

Examination Objectives

The objectives for reviewing the information system processing are to:

1. Determine if the corporate's policies, procedures, and internal controls are adequate to monitor and control data processing risk.

2. Determine that the corporate complies with the FCU Act, NCUA Rules and Regulations, NCUA issued Directives, the Accounting Manual for Federally Insured Credit Unions, and GAAP, as they directly or indirectly apply to information system processing.

3. Evaluate the adequacy of security policies relative to the risk to the institution.

4. Evaluate vendor management related security controls.

5. Assess the adequacy of the corporate's security controls.

6. Initiate corrective action when the corporate's internal IST controls, policies, procedures, and practices are deficient.

Examination Procedures

See Corporate Examination Procedures - Information Systems Processing (OCCU 303P).

Examination Questionnaire

See Corporate Examination Questionnaire - Information Systems Processing (OCCU 303Q).

References

1. Regulatory Handbook- Thrift Activities Volume I (OTC)

2. NCUA Rules and Regulations (Expanded Authorities Appendices)

3. FFIEC Information Technology Handbooks

4. OCCU Guidance Letters